UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/388,195	09/01/1999	EDWARD M. SCHEIDT	STS-127	3506

7590 05/17/2004

IP Strategies PC
1730 N. Lynn Street
Suite 500
Arlington, VA 22209

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	**PAPER NUMBER**
2131	13

DATE MAILED: 05/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/388,195	SCHEIDT, EDWARD M.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 April 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Detail Office Action

Claims 1-40 have been fully reconsidered and are pending.

Drawings

New corrected drawings are required in this application because the submitted drawings filed 4-2-04 do not comply with CFR 1.84. Specifically, the text is not clearly legible and uniform. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Response to Arguments

Applicant's arguments filed 4-2-04 have been fully considered but they are not persuasive. The arguments have been carefully considered but Examiner maintains all previous rejections.

On page 3 of the immediate response, Applicant argues that Lipner et al, hereafter, Lipner, "does not describe initializing the algorithm with a cryptographic key, and particularly not with a cryptographic key formed by combining splits." Examiner respectfully disagrees. Lipner discloses that a private key is generated from combined

components in column 13, lines 43-50 as one embodiment of his invention. The basis, or compliment of this private key is of coursed used to first encrypt an object in accordance with the well establish public key/private key algorithm. Also it is known that both the private and public keys are generated at the same time so one unlocks the other. Claim one explicitly discloses combining a plurality of key splits to generate a cryptographic key and initializing a cryptographic algorithm with the cryptographic key. This is the synonymous to creating a set of keys, public and private in which the private is formed from parts. Because the private key, KUpriv is consists of Kupriv1 and Kupriv2 and can be split and reconstructed the operation is commutative. One could just as easily create the two parts and combine them into one key or generate one key and divide them into two parts. Lipner also disclosing generating the parts first in column 14, lines 30-35. Examiner interprets the teachings of Lipner to suggest that a key can be formed and split and that two key can be created and joined in some fashion.

On page 3 of the immediate response, Applicant argues that Lipner does not disclose or suggest use of biometric correspondence to a cryptographic key split. As stated in the previous office action, Lipner does not explicitly disclose using biometric information as one of the part of the key. However, from the teaching in column 14, lines 30-35, the keys are generated and initialized (line 28) in parts. In column 10, lines 50-52, Lipner explicitly teaches that the keys can be seeded with externally generated parameters. One skilled in the art knows that and seed must be random. Only one individual knows a private key. In Lipner's invention the private key is split whereby at

least one split is still known only to the person or entity that created the key. Lipner also teaches that biometric are used to authenticate a person because they are hard to duplicate. A person's biometric data would be totally different and random from another person. Therefore one would be motivated to use such a personal way of creating a totally random key because it is very unlikely that another person can duplicate someone else's biometric data. From these teachings one of ordinary skill in the art at the time of the invention would have been motivated to modify the teachings of Lipner to include use a biometric device to generate a portion of the private key because it is an external random source of input.

In view of this, the Examiner maintains that the Lipner prior art teaches or suggests all of the limitations stated in the prior office action. Henceforth, the previous 35 USC 103 rejections still apply.

Claim Rejections - 35 USC § 103

Claims 1-6 and 21-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lipner et al (USP 5,991,406).

As per claim 1 and 21, Lipner et al teach both a method and computer apparatus for executing the disclosed method (column 7, line 35-40):

Combining a plurality of key splits to generate a cryptographic key (column 15, lines 13-16);

Initializing a cryptographic algorithm with a cryptographic key (column 7, line 40-43);

Applying cryptographic algorithm to an object [57].

Lipner et al fails to disclose using a biometric measurement as part of the encryption key. Lipner et al teach biometric tests are a way to authenticate a user (column 21, lines 34-41). Lipner et al teach that a key can be seeded with externally generated parameters (column 10, lines 50-52). In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Lipner et al to use biometrics as part of the key because it would add a personal parameter to the key that identifies who created it.

As per claims 2, 3, 22, and 23, Lipner et al teach adding a reference data (LEAF) and a key split (ELVS) to the encrypted message when sending it to the receiver (column 15, lines 31-32).

As per claims 4 and 24, Lipner et al teach retrieving key components (splits) from memory (column 10, lines 35-38).

As per claims 5, 6, 25, and 26, Lipner et al teach that encryption can be performed in hardware such as a PCMCIA card (smartcard) (column 5, lines 29-32). Because the encryption is done on a smartcard, it is inherent that the smartcard has storage capabilities necessary for performing the encryption. Furthermore, Lipner et al teach a system that can be executed in both hardware (i.e. smartcard) and software for

executing the disclosed method (column 7, line 35-40). Consequently, the combining of the key splits is inherently performed on a smartcard.

Claims 7, 8, 10-28, and 30-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia (USP 6,009,177) in view of Lipner et al.

As per claims 7, 14, 15, 16, 17, 27, 34, 35, 36, and 37 Sudia teaches:

Generating a private key by combining key spits (column 18, lines 65-67);

Initializing a cryptographic algorithm with a key (column 10, lines 62-67);

Encrypting an object according to cryptographic algorithm (see FIG. 5);

Adding combiner data (Message Control Header) (column 11, lines 33-39) which includes:

Reference data (FIG. 18);

Name data (FIG. 18);

Maintenance split (FIG. 18);

Maintenance level (FIG. 18);

Random split (column 18, lines 46-49);

Timestamp (FIG. 18);

Digital signature (FIG. 18);

Digital certificate (FIG. 18);

And storing the object with added combiner data (column 15, lines 39-43). Sudia teaches that the private key is broken up into splits (column 18, lines 12-15). Sudia teaches a random number is generated for each split and, consequently, a

random number is associated with each key (column 18, lines 12-61). Sudia is silent in disclosing that the key includes an organizational split, maintenance split, and a label split. Lipner et al teach that a key can be seeded with externally generated parameters (column 10, lines 50-52). Sudia teaches parameters to identify a user such as manufacturer's name (organization) (column 16, line 62), manufacturer public key/certificate (maintenance) (column 16, lines 60-61), and user's public signature (label) (column 17, line 15). Incorporating these parameters into the key splits to provide flexibility in the system's overall ability to enforce security. One skilled in the art would recognize that keys created from these parameters allow the system to authenticate a user and protect its resources from unauthorized persons. In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Lipner et al into the system of Sudia because it would allow the system to better protect its resources to users of varying trust and responsibility.

As per claims 8, 10, 28 and 30, the examiner supplies the same rationale for motivation for incorporating the teachings of Lipner et al into the system of Sudia as cited in the rejection of claim 7. Sudia teaches that various types of credentials are stored in memory for each user (column 16, line 31 – column 17, line 26). It is inherent that from these credentials is where the parameters will be selected to seed the key splits.

As per claims 11 and 31, Sudia teach that smart cards contain valuable user identification (column 22, lines 63-66). It would have been obvious to one of ordinary

skill in the art at the time of the invention to modify the system of Sudia by storing user information in the memory of a smart card.

As per claims 12 and 32, the examiner supplies the same rationale for motivation for incorporating the teachings of Lipner et al into the system of Sudia as cited in the rejection of claim 7. Sudia teaches adding combiner data (Message Control Header) (column 11, lines 33-39), which includes a timestamp (FIG. 18)

As per claims 13 and 33, the examiner supplies the same rationale for motivation for incorporating the teachings of Lipner et al into the system of Sudia as cited in the rejection of claim 7. Sudia teaches adding combiner data (Message Control Header) (column 11, lines 33-39), which includes an escrow certificate (FIG. 18), which includes a user name (I.D.) (FIG. 12).

As per claims 18 and 38, Sudia teaches encrypting the fields of the MCH (label reference data) (column 26, lines 10-14). It is inherent that the fields are encrypted before being added to the header because the same key encrypts not all of the fields. Sudia also teaches the creation of a new session key (second cryptographic key) by which the entire message can be decrypted. Sudia teaches that the private key is broken up into splits (column 18, lines 12-15). Sudia teaches that this key is created in part by a secret number (unique data instance) (column 26, lines 14-29). Sudia also teaches using a random number to help create strong keys (column 18, lines 44-60). Therefore the secret number could be random because random numbers are strong. Sudia teaches a random number is generated for each split and, consequently, a random number (split) is associated with each key (column 18, lines 12-61).

As per claims 19, 20, 39, and 40, Sudia teaches that part of the header data is encrypted (see FIG. 18, and specifically the sender's escrow certificate number (column 23, lines 27-31)). Sudia teaches adding combiner data (Message Control Header) as a header to all packets (column 11, lines 33-39).

Claims 9 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia and Lipner et al as applied to claims 7, 8, 27, and 28 above, and further in view of Nguyen (USP 5,689,566).

As per claims 9 and 29, Sudia teaches encrypting the fields of the MCH (label reference data) (column 26, lines 10-14). Sudia also teaches the creation of a new session key (second cryptographic key) by which the entire message can be decrypted. Sudia teaches that this key is created in part by a secret number (unique data instance) (column 26, lines 14-29). Sudia also teaches using a random number to help create strong keys (column 18, lines 44-60). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Sudia to include the random number into the generation of the second key.

The combined teachings of Sudia and Lipner et al are silent in disclosing creating a key in part from a user ID and password. Nguyen teaches creating a key from a user ID and password (column 3, lines 63-64). Sudia teaches that the private key is broken up into splits (column 18, lines 12-15). Creating part of the key from the user's ID and password allows the system to know who created the key (someone who knows both a valid user ID and the password for that user). In view of this, it would have been

obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Nguyen into the combined system of Sudia and Lipner et al because it would decrease the chance of an unauthorized person of gaining system resources.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Michael R Vaughan
Examiner
Art Unit 2131

MV

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100